REMARKS

In response to the Office Action mailed July 24, 2007, Applicants respectfully request reconsideration. To further the prosecution of this Application, Applicants submit the following remarks, have canceled claims and have added new claims. The claims as now presented are believed to be in allowable condition.

Claims 1, 5, 7, 10-17, 21-22, 24-32, and 36-42 were pending in this Application. By this Amendment, claims 1, 5, 7, 10-16, 21-22, 24-31, 36, and 39-42 have been canceled. Applicants expressly reserve the right to prosecute at least some of the canceled claims and similar claims in one or more related Applications. Claims 43-52 have been added. Accordingly, claims 17, 32, 37-38, and 43-52 are now pending in this Application. Claims 17, 32, 37, 38, and 51 are independent claims.

Election/Restriction

Applicant hereby affirms the election of Group III without traverse, namely, claims 17, 32 and 37-38.

Rejections under §103(a)

Claims 37 and 38 (claims 37 and 38 were incorrectly referenced as 38 and 39, respectively, on page 2 of the Office Action) were rejected under 35 U.S.C. §103(a) as being unpatentable over U.S. Patent Publication No. 2003/0226023 (Peters) in view of U.S. Patent No. 6,081,206 (Kielland). Claims 37 and 38 (claims 37 and 38 were incorrectly referenced as 38 and 39, respectively, on page 7 of the Office Action) were also rejected under 35 U.S.C. §103(a) as being unpatentable over Peters in view of U.S. Patent No. 6,397,334 (Chainer, et al.). Claims 17 and 32 were rejected under 35 U.S.C. §103(a) as being unpatentable over Peters and Kielland in further view of U.S. Patent No. 5,517,568 (Grube, et al.). Claims 17 and 32 were also rejected under 35 U.S.C. §103(a) as being unpatentable over Peters and Chainer in further view of Grube.

Applicants respectfully traverse each of these rejections and request reconsideration. The claims are in allowable condition.

Peters teaches a technique for deterring theft of media recording devices (Abstract). A media file recorded by a recording device is encrypted, so that it cannot be properly played back without a cryptographic key supplied to the owner of the device (Paragraph 0023). Because asymmetric public key encryption is more secure but also more complex (and therefore slower) than symmetric shared key encryption, a symmetric key may be used to encrypt the media files while the symmetric key is encrypted using public key encryption. (Paragraph 0031). In order to aid a customer who has lost his or her key to a device, a manufacturer may provide a key escrow service to give a customer the key upon presentation of some proof of ownership of the device (Paragraph 0043).

Chainer discloses a system and method for authenticating an image of an object (Abstract). An object 102 contains one or more tags 101, such as RFID tags, which are not functionally removable from the object 102 (Col. 3, line 63 through Col. 4, line 8). A tag reader 103 (such as an RFID tag reader) reads the RFID tags 101 as a coupled camera system 104 records an image of the object 102 (Col. 4, lines 27-36). A composite generator 105 combines the image and the sensed RFID results to encode the tag ID information together with a hash of the image (Col. 4, lines 37-48). This encoded data may be encrypted for further security (Col. 5, lines 43-54). In addition, other measuring devices 400 may record additional properties of an object 406 in order to provide additional information with which to identify an object (Col. 6, lines 17-38). In addition, a zoom lens 108 may be used to take multiple pictures of an object 102 with different settings (Col. 6, lines 39-45).

Grube discloses a method for detecting unauthorized use of a communication unit 102 in a secure wireless communications system 100 (Col 2, lines 44-45). If a communication unit 102 sends an encrypted communication encrypted with inactive, previously used, encryption parameters (such as a inactive encryption key), then this is detected by system manager 110 (Col. 3, lines 21-36), and the communication unit 102 is flagged as an unauthorized unit (Col. 4, lines 48-60).

Claims 16-17

Claim 17 (which has now been placed into independent form by incorporating all the limitations previously found in base claim 16) recites a method for generating an output signal from a video data acquisition system. The method includes (a) receiving a video signal that varies depending on sensed images, (b) encrypting the video signal using a first key, (c) encrypting the first key using a second key, (d) including at least the encrypted first key and encrypted video signal in the output signal, (d) implementing a recognition algorithm to identify objects associated with the sensed images, (e) in response to recognizing an object, embedding encrypted data information identifying the recognized object in the output signal, and (f) randomly generating a new encryption key for encrypting different portions of the video signal over time.

The cited references to do not teach or suggest, either alone or in combination, a method including (a) receiving a video signal that varies depending on sensed images, (b) encrypting the video signal using a first key, (c) encrypting the first key using a second key, (d) including at least the encrypted first key and encrypted video signal in the output signal, (d) *implementing a recognition algorithm to identify objects associated with the sensed images*, (e) *in response to recognizing an object, embedding encrypted data information identifying the recognized object in the output signal*, and (f) *randomly generating* *a new encryption key for encrypting different portions of the video signal over time.*

Peters teaches a technique for deterring theft of media recording devices in which an asymmetric key may be used to encrypt a symmetric key which was used to encrypt video data recorded by a media device. However, Peters does not teach (i) *implementing a recognition algorithm to identify objects associated with the sensed images*, (ii) *in response to recognizing an object, embedding encrypted data information identifying the recognized object in the output signal*, and (iii) *randomly generating a new encryption key for encrypting different portions of the video signal over time.*

The Office Action, on page 8, cites Chainer (Figs. 2-3, Col. 4, line 30 through Col. 6, line 17, and Col. 7, lines 52-61) as teaching features (i) and (ii). However, the cited portion of Chainer does not teach *implementing a recognition algorithm to identify objects associated with the sensed images*, and *in response to recognizing an object, embedding encrypted data information identifying the recognized object in the output signal.* Rather, Chainer teaches using an RFID tag reader 103 or other measuring device 400 to record additional data (e.g., a time stamp, focal length, hash of the image, interferometric measurements, biometric data), but not a *recognition algorithm to identify* an object from a sensed image. No *recognition* is performed in Chainer. The additional data is merely recorded as a watermark or signature with a recorded image. The additional data may later serve to verify the identity of the recorded image, but in any event, Chainer does not teach *in response to recognizing an object, embedding encrypted data information identifying the recognized object in the output signal* – indeed, any identity verification takes place subsequent to recording the additional data. If the rejection of claim 16 is to be maintained, Applicants respectfully request that it be pointed out with particularity where the cited prior art teaches such *implementing* of *a recognition algorithm to identify objects associated with the sensed images*, and *in response to recognizing an* *object, embedding encrypted data information identifying the recognized object in the output signal*. Thus, claim 17 patentably distinguishes over Peters in view of Chainer, and the rejection of claim 17 under 35 U.S.C. §103(a) should be withdrawn.

The Office Action, on pages 12 and 13, cites Grube (Col. 1, lines 51-67) as teaching feature (iii). However, the cited portion of Grube does not teach *randomly generating a new encryption key for encrypting different portions of the video signal over time*. Rather, the cited portion of Grube teaches regularly changing the active system encryption parameters (including the encryption algorithm and encryption key) within a secure wireless communication system to maintain security over a long period of time (Col. 1, lines 51-67). However, the cited portion does not teach *randomly* generating a *new* encryption key, nor does it teach using a new encryption key for encrypting *different portions of* a *video signal over time*. That is, the cited portion could be referring to a pre-provided set of encryption keys that are not *generated* as part of the method. Also, even if the keys were generated, the cited portion would not teach generating the new keys *randomly* – they could instead be calculated based on a specific pattern. Also, while the cited portion teaches changing the encryption key regularly, it does not teach using the changed keys *for encrypting different portions of* a *video signal over time* – the cited portion could be limited to encrypting separate signals with different keys and not encrypting one (video or other) signal with multiple keys over time. Thus, claim 17 patentably distinguishes over Peters in view of Chainer and Grube, as well as over Peters in view of Kielland and Grube, and the rejection of claim 17 under 35 U.S.C. §103(a) should be withdrawn.

For the reasons stated above, claim 17 patentably distinguishes over the cited prior art, and the rejection of claim 17 under 35 U.S.C. §103 should be withdrawn. Accordingly, claim 17 is now in allowable condition.

Claims 31-32

Claim 32 (which has now been placed into independent form by incorporating all the limitations previously found in base claim 31) recites an apparatus to support surveillance. The apparatus includes a camera to generate a video signal that varies depending on sensed images. It also includes a memory device to store at least first and second encryption keys and a processor that encrypts the video signal using the first encryption key. The processor encrypts the first encryption key with the second encryption key and produces an output signal including at least the encrypted video signal and the encrypted first encryption key. The apparatus also includes a recognition system to identify objects associated with the sensed images, the processor embedding encrypted data information identifying the recognized object in the output signal. The apparatus also includes an encryption key generator that randomly generates a new value for the first encryption key to uniquely encrypt different portions of the video signal over time.

The cited references to do not teach or suggest, either alone or in combination, an apparatus having the claimed features. The claimed features are similar to those found in claim 17. Accordingly, claim 32 distinguishes over the prior art for reasons similar to those presented above in connection with claim 17. For the reasons stated above, claim 32 patentably distinguishes over the cited prior art, and the rejection of claim 32 under 35 U.S.C. §103 should be withdrawn. Accordingly, claim 32 is now in allowable condition.

Claims 37-38

Claims 37 and 38 have been amended to incorporate an additional limitation (with support in the Specification, for example, at page 18, line 3 through page 19, line 7) which patentably distinguishes them from the prior art. The prior art does not teach using a *third encryption key to encrypt the data* *identifying objects associated with the sensed images*, the *third key being distinct from the first key*. Therefore, the rejections of claims 37 and 38 under 35 U.S.C. §103 should be withdrawn. Accordingly, claims 37-38 are now in allowable condition.

Newly Added Claims

Claims 43-52 have been added and are believed to be in allowable condition. Claims 43-44 depend from claim 17. Claims 45-46 depend from claim 32. Claims 47-48 depend from claim 37. Claims 49-50 depend from claim 38. Claim 52 depends from claim 51. Support for claims 43, 45, 48, 50, and 52 is provided within the Specification, for example, on page 15, line 22 through page 16, line 11. Support for claims 44 and 46 is provided within the Specification, for example, on page 18, line 3 through page 19, line 7. Support for claims 47 and 49 is provided within the Specification, for example, on page 17, lines 9-18 and page 19, line 17 through page 20, line 3. Support for claim 51 is provided within the Specification, for example, on page 28, lines 4-10 and 35-29, and on page 18, line 3 through page 19, line 7. No new matter has been added.

Conclusion

In view of the foregoing remarks, this Application should be in condition for allowance. A Notice to this affect is respectfully requested. If the Examiner believes, after this Amendment, that the Application is not in condition for allowance, the Examiner is respectfully requested to call the Applicants' Representative at the number below.

Applicants hereby petition for any extension of time which is required to maintain the pendency of this case. If there is a fee occasioned by this Amendment, including an extension fee, that is not covered by an enclosed check, please charge any deficiency to Deposit Account No. 50-3661.

If the enclosed papers or fees are considered incomplete, the Patent Office is respectfully requested to contact the undersigned collect at (508) 616-2900, in Westborough, Massachusetts.

Respectfully submitted,

/Michael Ari Behar/

M. Ari Behar, Esq.
Attorney for Applicants
Registration No.: 58,203
Bainwood, Huang & Associates, L.L.C.
Highpoint Center
2 Connector Road
Westborough, Massachusetts 01581
Telephone: (508) 616-2900
Facsimile: (508) 366-4688

Attorney Docket No.: 1004-120

Dated: October 24, 2007